TMA Privacy Office Information Paper

Records Management • FOIA • DUAs • HIPAA Compliance • ADP Security • Privacy Act • System of Records • PIAs

Security Awareness and Training

HIPAA Security • November 2003

Standard Requirement

As part of their administrative safeguards, covered entities must develop a security awareness and training program. Like the privacy training, this standard requires that all members of a covered entity's workforce participate in the program. Awareness and training are considered to be separate activities. Security "awareness" exists to continuously heighten the workforce members' familiarity with security. This is done through posters, email reminders, etc. "Training," on the other hand, functions as a way to teach someone security practices. Covered entities should also maintain records documenting implementation of their security awareness and training program.

This standard includes four component implementation specifications, all of which are addressable:

- security reminders,
- protection from malicious software,
- log-in monitoring, and
- password management.

Implementation Specifications

The first implementation specification, security reminders, is an effective means to increase security awareness and strengthen a covered entity's security position. Periodic security updates help to raise and maintain awareness. Security reminders include e-mail messages, newsletters, posters, etc. As part of a covered entity's security risk assessment, they should evaluate the need for policies and procedures to make their staff aware of security concerns on an ongoing basis. Covered entities should also maintain records documenting implementation of their security awareness plan.

The second implementation specification, protection from malicious software, evaluates the need for policies and procedures to inform all users of electronic protected health information (EPHI) of the threat of malicious software. A way to inform all users of threats could be through security reminders. Covered entities should prepare and document in their risk management plan, appropriate procedures for

Security Awareness and Training

to virus detection. Covered entities should also maintain records documenting implementation of their malicious software education plan.

The third implementation specification includes procedures for monitoring log-in attempts and reporting discrepancies. The log-in screen on many operating systems displays information concerning past log-in attempts including the user name last used during log-in, the date and time of the last successful log-in and the number of unsuccessful log-in attempts since the last successful log-in. This information can alert users to possible unauthorized access attempts from that workstation. As part of their information security risk assessment, covered entities should assess the value of training personnel to monitor and report log-in discrepancies. If the risk assessment indicates this safeguard is appropriate, covered entities should include policies and procedures describing this training in their risk management plan. The security management process standard contains a related requirement within its information system activity review component.

The last implementation specification implements procedures for creating, changing, and safeguarding passwords. In their risk assessment, covered entities should assess the value of training personnel in the organization's password policies and how to create, change, and protect passwords. If the assessment indicates this safeguard is appropriate, covered entities should include policies and procedures describing password training in their risk management plan. Some covered entities do not use a password as a form of authentication. If they use other authentication approaches, those approaches would have similar safeguards and training needs.

Because all of these implementation specifications are addressable, covered entities have some leeway in how they implement the standard. The "amount and timing of training should be determined by each covered entity; training should be an evolving, on-going process in response to environmental and operational changes...." (Final Rule, pp.8350). Security awareness training is also required for workforce members who may only work on the site for a limited time period. Business Associates, however, are not required to

Security Awareness and Training

HIPAA Security◆November 2003

participate in security training. According to DHHS, Federal agencies must all have security awareness training.

This is due to the requirements of the Government Information Systems Reform Act (GISRA).

See also:
45 CFR 164.308(a)(5)
National Institute of Standards and Technology, Information Technology Security Training Requirements (NIST SP 800-16, April 1998)

Federal and DoD regulations that support this standard
OMB A-130 App. III
DoD 8510.1-M
DoDD 8500.1
DoDI 8500.2

TMA Privacy Office Information Paper

Records Management◆FOIA◆DUAs◆HIPAA Compliance◆ADP Security◆Privacy Act◆System of Records◆PIAs